MYRA

WHITEPAPER

DORA: Harmonized regulatory framework for greater cybersecurity in the EU financial sector increases compliance hurdles

Executive Summary

The financial sector relies heavily on information and communication technology (ICT) – not least because of the steadily increasing demand for digital services. This makes banks and financial service providers particularly vulnerable to cyber incidents, which are considered the biggest risk factor for the financial industry. Digital operational resilience is therefore essential.

In order to increase cyber resilience, supervisory authorities are relying on an increasingly tighter regulatory framework. So too is the EU – the Digital Operational Resilience Act (DORA) is designed to ensure, on the one hand, that all financial sector stakeholders have taken the necessary security precautions to prevent or mitigate ICT-related cyber incidents. On the other hand, DORA is intended to harmonize the requirements necessary for this across the EU.

Higher compliance hurdles due to DORA

DORA contains new or more specific provisions relating to governance, ICT risk management, classification and reporting of ICT-related incidents, testing of digital operational resilience (resilience tests), management of risk by ICT third-party service providers, and information-sharing arrangements.

This results in new challenges and numerous additional burdens for financial entities because they have to review their processes and adapt them to the extended requirements compared with national regulations such as MaRisk and BAIT. This applies in particular to cooperation with ICT third-party service providers.

Third-party service providers put to the test

DORA introduces a supervisory framework for the direct monitoring of critical ICT service providers operating in the financial sector. In order to avoid potential penalties, financial entities must ensure that all requirements – such as those relating to risk assessment, reporting obligations, and audit rights – are implemented correctly. For this reason, a re-evaluation, including risk analysis, of existing outsourcing partners is recommended.

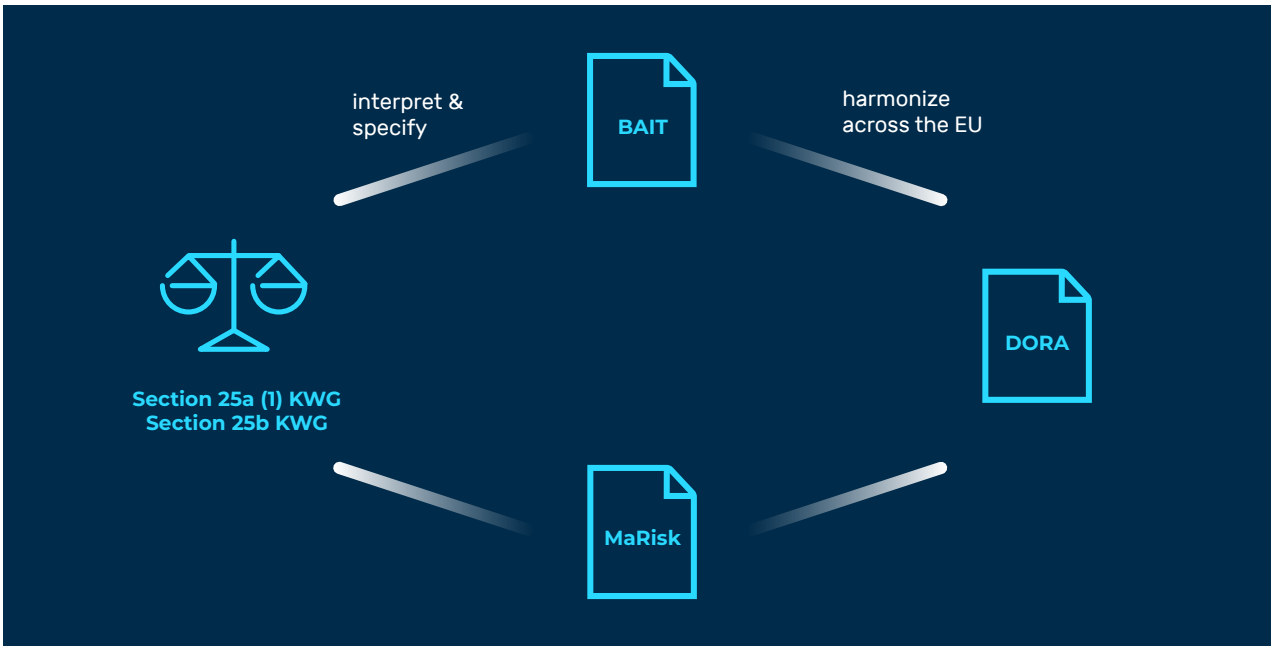
Choice of service provider is crucial

With the support of highly specialized and certified service providers, financial entities will be able to master the compliance hurdles associated with DORA without much additional effort. Moreover, anyone who wants absolute legal certainty in data protection and contract data processing following the discontinuation of the Privacy Shield agreement should choose a provider from the EU. This ensures that all regulatory requirements for IT security, data protection, and compliance are met in full.

Initial situation: Tighter regulatory framework poses new challenges for the financial industry

The financial industry has always been the focus of criminals. In the past, masked criminals stormed into banks at gunpoint to steal gold and cash. Today, cybercriminals are targeting valuable digital assets. According to Boston Consulting Group[1], banks and financial services companies are 300 times more likely to be the target of cyber attacks than other businesses. Allianz even lists cyber incidents as the biggest risk factor for the financial industry in its Risk Barometer 2023[2].

Against this backdrop, banks must continuously improve their cyber resilience and IT security, just as they protect themselves from robbery with armored vehicles, vaults, and guards. Supervisory authorities are responding to the digital transformation with a tighter regulatory framework that demands greater commitment from institutions in terms of IT security, data protection, and compliance.



MaRisk and BAIT both interpret and specify the statutory requirements of the German Banking Act (KWG, Section 25a (1) and Section 25b). The objective of DORA is to define overarching uniform requirements for the financial industry. The existing regulation is to be harmonized at European level while maintaining proportionality.

DORA introduces a comprehensive legal framework at EU level, which contains new or more specific rules on digital operational stability for all supervised financial institutions.

The legal act is part of a package of measures to digitize the financial sector, with which the Commission aims to promote Europe's competitiveness and innovation in the financial sector. In addition to greater cybersecurity, DORA promises a level playing field for all financial service providers in the European single market – in line with the principle of "same activity, same risks, same rules". DORA is designed to ensure that the same regulatory requirements apply to companies in the financial sector throughout Europe.

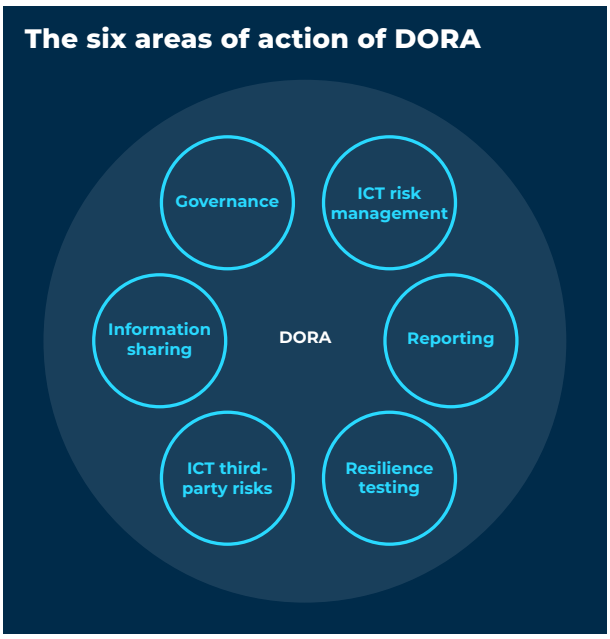
Specifically, DORA aims to harmonize the rules for ICT risk management and the classification and reporting of ICT incidents across the EU. Moreover, EU-wide standards for digital operational resilience tests will be defined in order to better identify as yet unknown vulnerabilities and risks. In addition, DORA breaks new ground in monitoring service providers with a supervisory framework for critical ICT third-party service providers.

1 Boston Consulting Group - Global Wealth 2019 - Reigniting Radical Growth
2 Allianz Global Corporate & Specialty - Allianz Risk Barometer 2023

Financial entities need to readjust IT security and compliance

On the basis of the current DORA draft, it can be assumed that financial entities will be faced with further IT requirements that go beyond existing regulations such as MaRisk or make them more stringent. For many banks and financial service providers, the planned changes will therefore mean considerable additional work. They will have to review their processes relating to governance, ICT risk management, reporting, resilience testing, third-party ICT risks, and information exchange and adapt or restructure them as necessary.

New EU reporting regulations, for example, require the provision of root cause analysis reports no later than one month after a major ICT incident occurs. The development of response and recovery plans is mandatory. The DORA regulations also have a direct impact on collaboration with ICT service providers such as cloud computing providers.



Technical standards as guidelines for compliance

While DORA does not provide for the standardization of specific ICT systems, tools, or technologies, it does require the appropriate application of European and internationally recognized technical standards (e.g., ISO) or industry best practices. These include, for example, the ISO 27000 family or ISO 27001 developed by the German Federal Office for Information Security (BSI) on the basis of IT-Grundschutz (IT baseline protection). Both deal with the design of an information security management system (ISMS) and the introduction of all necessary security measures.

An ISMS operated in accordance with these standards makes it possible to identify potential threats at an early stage and mitigate them by means of tailor-made countermeasures. This enables companies to ensure the confidentiality, availability, and integrity of any and all information. However, ISO 27001 certification alone is not a free pass for DORA compliance.

Check cooperation with third-party service providers

The European Supervisory Authorities (ESAs) will, among other things, develop Technical Regulatory Standards (RTS) for the monitoring of risk by ICT third parties – these are to be submitted by the ESAs to the Commission by January 17, 2024. This will force some institutions to look for new outsourcing partners, as it is foreseeable that only highly specialized and certified providers will be able to meet the RTS. In this context, the German banking industry expects even greater regulatory density and depth.[3]

3 https://die-dk.de/media/files/20201214_DK-Positionen_DORA.pdf

Key objectives of DORA: Increased cyber resilience and EU-wide harmonization of the requirements needed to achieve it

The consequences of a cyber attack or disruption at an important cross-border financial service can have far-reaching effects on other companies, sub-sectors, or even the rest of the economy. That is why digital operational resilience in the financial sector is of crucial importance. The EU Commission still sees a need for improvement here and has identified some problems that DORA is intended to solve:

Problem from the EU standpoint	Intended solution
High dependency on ICT makes financial entities vulnerable to cyber attacks	Strengthen cyber resilience through new or more specific requirements
Fragmented and inconsistent national compliance rules	Reduce fragmentation and national special paths through EU-wide harmonization
High regulatory burden for European-wide financial entities due to lack of legal clarity	Rechtliche Klarheit zu Vorschriften für digitale Resilienz schaffen
Lack of uniform reporting requirements complicates the work of supervisory authorities	Klassifizierung und Meldung von IKT-bezogenen Vorfällen vereinheitlichen
Regulators cannot directly monitor outsourced services	Aufsichtsrahmen zur direkten Überwachung kritischer IKT-Dienstleister einführen

> *Harmonizing the various European regulatory approaches to the security of financial IT, which the draft DORA seeks to do, is a necessary step toward improving cyber resilience in the financial sector.*

Bundesverband deutscher Banken e.V. (Association of German Banks)

One regulation for everyone

DORA applies to all financial entities regulated at the EU level, from credit, payment, and e-money institutions to insurance companies and credit rating agencies. In addition, the new regulation also affects ICT third-party service providers that provide services in the financial sector.

DORA addresses the entire financial industry and associated ICT third-party service providers

When do the DORA regulations go into effect?

The final version of DORA came into effect on January 16, 2023. The requirements formulated therein for all affected financial companies take effect immediately, but are not enforceable until 24 months after entry into force. Companies and institutions therefore have two years to implement the new requirements. In parallel, the ESAs will draw up technical standards to specify the application of the new rules.

In focus: Impact of DORA on the outsourcing of ICT services

Among other things, DORA will lead to adjustments in existing national regulations on outsourcing such as MaRisk and BAIT. Under the current draft of DORA, EU financial entities must assess the risk of outsourcing in advance and conduct due diligence to identify suitable third-party service providers. In addition, Article 28, Section 6 states: Financial entities may only enter into contractual arrangements with ICT third-party service providers that comply with appropriate information security standards. When those contractual arrangements concern critical or important functions, financial entities shall, prior to concluding the arrangements, take due consideration of the use, by ICT third-party service providers, of the most up-to-date and highest quality information security standards. In addition, contracts with third-party service providers must be thoroughly reviewed by analyzing subcontracting in order to avoid concentration risks.

Contractual arrangements with third-country service providers must take into account data protection, effective enforcement of the law, insolvency provisions in the event the third-party service provider becomes insolvent, and restrictions that may arise in relation to the urgent restoration of company data.

Oversight framework: New approach to oversight of critical ICT third-party service providers

One major innovation is the planned oversight framework for critical ICT third-party service providers. It specifies that in the future, these will be directly controlled by one of the ESAs. The respective lead ESA can then also request information, conduct external and on-site inspections of the service providers, issue recommendations and instructions, and impose fines (up to one percent of the daily worldwide turnover) or even order contract terminations in the event of non-compliance. Whether an ICT third-party service provider is classified as critical is decided by the Joint Committee of the ESAs on the basis of a list of criteria set out in DORA.

Third-party service providers will therefore have to adjust to stricter regulation. However, the ESAs' new supervisory options do not exempt financial entities from their regulatory responsibility for the ICT service providers they use. Those who outsource services must still ensure that all the requirements defined in DORA for risk management and monitoring of the contractual arrangements concluded with critical ICT third-party service providers are met.

Important contractual provisions

Article 30 of DORA prescribes a number of provisions for contractual agreements on the use of ICT services. Among other things, contracts must cover these subject areas:

- Type & scope of the ICT service
- Location(s) of service provision
- Data protection specifications
- Emergency support requirements
- Cooperation obligation with competent authorities
- Contingency plans
- TLPT (Threat-Led Penetration Test)
- Audit rights
- Termination rights
- Obligation to participate in awareness training
- Exit strategies

DORA requirements force companies to rethink their service provider choices

Only a few highly specialized and certified third-party service providers can fully meet DORA's stringent requirements. Financial entities should make sure to carefully check whether their current service provider is one of them.

The supervisory authorities are now taking a much closer look, especially when it comes to data protection and contract data processing. Service providers – like the financial entities themselves – must correctly implement all the provisions of the European General Data Protection Regulation (EU GDPR). Ultimately, only European partners can do this. In practice, the strict requirements will be much easier to implement by choosing a certified third-party service provider from the EU. Here, financial entities can be sure that all requirements in terms of security, data protection, and compliance are fully met.

From the outset, ICT third-party service providers without a commercial presence in the EU whose operating failure would have a systemic impact on the provision of financial services are excluded as outsourcing partners. Against this background, it is advisable for financial entities to re-evaluate their outsourcing partners – including a risk analysis of the contractual partners – and to prepare early on for a change of service provider that may become necessary.

Legal uncertainty for non-European partners

With the discontinuation of the Privacy Shield agreement for transatlantic data transfers between Europe and the USA, cooperation with US providers is on shaky ground. Legally secure data transfers are difficult to implement due to the conflicting positions of the European GDPR and US law. The new standard contractual clauses adopted by the EU Commission at the beginning of June do nothing to change this situation because they do not conclusively resolve any conflicts with the national laws of third countries. One particular obstacle in this context is the US CLOUD Act, which compels internationally operating American companies to hand over data if US authorities request it. Such hurdles can be avoided by choosing local providers subject to European jurisdiction.

Overview: The key requirements of DORA for banks and financial service providers

Many of the requirements formulated in DORA[4] are already known in principle from existing regulations for the financial sector, such as the EBA guidelines, MaRisk, or BAIT, and are already being implemented in practice. This applies, for example, to the involvement of the management body, the appointment of outsourcing officers, the development of crisis communication plans, and the management and classification of incidents. There is no additional burden here for most financial entities.

In some cases, however, the DORA requirements go beyond or strengthen the requirements of MaRisk, etc. This applies, for example, to the area of ICT risk management (including risk management frameworks, identification, protection and prevention, detection of anomalous activities, as well as countermeasures and recovery), the supervision of ICT third-party service providers, and the auditing of ICT systems.

In addition, instead of a principle-based approach, DORA follows a rule-based approach with concrete targets for achieving the objectives. The regulatory technical standards yet to be developed by the ESAs will set out detailed implementation methods, leaving banks and financial services providers with less room for maneuver compared with the existing regulations.

In view of the planned direct controls of ICT third-party service providers by the ESAs, financial entities will also have to check whether their service providers are at all able to implement the strict requirements (see focus topic on page 7). The following pages provide a concise overview of the key requirements of DORA.

4 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32022R2554

Governance and organisation

- **Strong involvement of the management body:** The management body defines, approves, oversees, and is accountable for the implementation of all arrangements related to the ICT risk management framework. This includes determining the risk tolerance level, setting clear roles and responsibilities, allocating appropriate budgets, approving audit, business continuity and disaster recovery plans, and reviewing arrangements with ICT third-party service providers.
- **Appointment of an outsourcing officer:** Financial entities shall establish a role or designate a member of senior management to monitor and document the arrangements concluded with ICT third-party service providers.
- **Training requirements:** In order to be able to understand and assess ICT risks and their impact on operations, members of the management body are required to follow regular specific training.

ICT risk management

- **ICT risk management framework:** Financial entities shall have an ICT risk management framework that enables them to address ICT risk quickly, efficiently, and comprehensively. The operational resilience thus ensured must match the business needs, size, and complexity of the financial entity. DORA supplements or more precisely specifies the requirements of MaRisk, etc.
- **Identification:** Financial entities shall identify, classify, and document business functions and information assets supporting these functions that are potential sources of ICT risk. This applies in particular to system configurations that are interconnected with internal and external ICT systems. Those that do not qualify as microenterprises shall perform a specific ICT risk assessment on all legacy systems on a regular basis, but at least yearly.
- **Protection and prevention:** The functioning of ICT systems shall be continuously monitored and controlled to ensure adequate protection. This requires the preventive implementation of adequate security strategies, policies, procedures, and tools.
- **Detection:** Financial entities shall have in place mechanisms to promptly detect anomalous activities and identify all potential single points of failure. This will lead to additional burdens compared to MaRisk.
- **Response and recovery:** Financial entities shall put in place response and recovery measures as well as develop appropriate business continuity and disaster recovery policies and plans. Even companies that otherwise already meet many of DORA's ICT risk management requirements should therefore consider whether their response and recovery policies and plans also comply with the extended rules in these areas.
- **Communication:** Financial entities shall develop a crisis communication plan that enables" a responsible disclosure of ICT-related incidents or major vulnerabilities" to clients, counterparts, and the public.

ICT-related incident management, classification and reporting

- **ICT-related incident management process:** Financial entities shall establish and implement a specific incident management process to identify, track, log, categorize, and classify ICT-related incidents.
- **Classification of ICT-related incidents and cyber threats:** The classification of ICT-related incidents shall be based on a number of criteria to be further developed by the Joint Committee of the ESAs.
- **Reporting of major ICT-related incidents and voluntary notification of significant cyber threats:** Companies are required to report major ICT incidents to the competent authority within prescribed time limits and using harmonized reporting templates.

Digital operational resilience testing

- **General requirements for the performance of digital operational resilience testing:** As an integral part of the ICT risk management framework, DORA requires financial entities to adopt a sound and comprehensive digital operational resilience testing program covering ICT tools, systems, and processes. The program shall include a full range of appropriate testing methodologies, including open source software analyses, network security assessments, gap analyses, physical security analyses and reviews, scanning software solutions, compatibility testing, performance testing, end-to-end testing, and penetration testing. All critical ICT systems and applications must be tested at least yearly.
- **Advanced testing of ICT tools, systems and processes based on TLPT:** Certain financial entities shall carry out advanced audits of their ICT tools, systems, and processes using threat led penetration testing (TLPT) based on TIBER-EU[5] at least every three years. These tests provide a realistic check of a company's cyber resilience under controlled conditions.
  The aim is to identify and subsequently eliminate vulnerabilities in critical systems, organisational structures, and processes. To this end, red teaming service providers carry out attacks on productive systems on the basis of a specific threat analysis, imitating the methods currently employed by real attackers. The operational units under attack are not aware of the tests and attempt to fend off the attacks using all available means. The advanced tests go beyond what MaRisk, etc. require. Affected companies should therefore closely monitor how the ESAs establish the implementation criteria.

Management of ICT third-party risk

- **General principles:** Financial entities shall manage ICT third-party risk within their ICT risk management framework in accordance with certain principles. These include responsibility and liability, proportionality, a strategy for ICT third-party risk, documentation and record-keeping, pre-contractual analysis, information security, audits and inspections, termination rights, and exit strategies. The proposed oversight framework does not replace and does not supersede in any form or for any aspect financial entities' management of the risk inherent in their use of ICT third-party service providers.
- **Preliminary assessment of ICT concentration risk at entity level:** The mandatory preliminary assessment by the financial entities aims to determine whether the conclusion of a contractual arrangement in relation to the ICT services would lead to a contract with an ICT third-party service provider considered dominant, which is not easily substitutable. It should also show whether several contractual arrangements have been concluded with the same ICT third-party service provider or with closely connected service providers. This is intended to avoid concentration and lock-in risks.
- **Key contractual provisions:** The rights and obligations of the financial entity and of the ICT third-party service provider shall be clearly allocated and defined in a contractual arrangement whose detailed scope is defined in legislation.

Information-sharing arrangements

- **Information-sharing arrangements on cyber threat information and intelligence:** DORA aims to establish a European standard that enables financial entities to voluntarily share cyber threat information and intelligence with each other to strengthen digital operational resilience. This includes indicators of compromise, tactics, techniques, procedures, cybersecurity alerts, and configuration tools.

5 https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html

The bottom line: Service providers take a central role in managing the added burden of the DORA regulatory framework

The implementation of EU-wide security standards, harmonized testing, and uniform reporting structures envisaged by DORA is a necessary step toward strengthening cyber resilience in the European financial sector. After all, the more the day-to-day business of banks and financial service providers shifts to digital environments, the more important it becomes to safeguard against cyber threats. The supervisory authorities have also recognized this.

> *[…] IT governance and information security now have the same priority for the supervisory authority as providing institutions with capital and liquidity.*
>
> *German Federal Financial Supervisory Authority (BaFin)*

This results in a stricter and more extensive regulatory framework, which creates ever higher compliance hurdles. For banks and financial service providers, DORA means a significant additional burden overall: they will have to deal more intensively than ever with their IT architecture and compliance issues and review and adapt in detail the measures already taken under MaRisk and BAIT.

DORA brings a significant innovation in the area of cooperation with third-party providers. Here, institutions must scrutinize and reassess their ICT service providers in any case to ensure that all DORA requirements are met. Service providers specializing in cybersecurity with technological know-how, the relevant certifications, and expertise in outsourcing/compliance for the financial sector can provide effective support here. With their help, financial entities will be able to meet all regulatory requirements without much in-house effort and cover their cybersecurity, performance, and compliance needs in equal measure.

This makes Myra the perfect partner for the financial industry

- Myra meets all of DORA's key requirements for risk management, reporting, testing, and outsourcing
- Audit-proof: Myra meets all requirements for material outsourcing according to Section 25b of the Banking Act (KWG), MaRisk AT9, and BAIT.
- Investment-secure technology: fully automated attack mitigation, high-performance delivery, maximum scalability.
- GDPR-compliant specialist provider with industry expertise
- Maximum certified quality: ISO 27001 based on IT-Grundschutz (IT baseline protection), PCI-DSS certified, BSI-KRITIS certified, BSI C5 attestation (in progress), Trusted Cloud.

First-class service quality thanks to certified security

As a specialist provider in the financial sector and other sensitive areas, it goes without saying that Myra meets the same stringent requirements as our customers. Myra's comprehensive certifications ensure that our customers achieve the maximum in security and compliance. Myra is the highest certified provider on the market and the only one in the world to meet all 37 criteria of the Federal Office for Information Security (BSI) for qualified service providers for critical infrastructure (KRITIS). We thus set the standard in IT security.

Zertifiziert vom Bundesamt für Sicherheit in der Informationstechnik (BSI) nach ISO 27001 auf Basis von IT-Grundschutz | Zertifiziert nach Payment Card Industry Data Security Standard | KRITIS-qualifiziert nach §3 BSI-Gesetz| Konform mit der (EU) 2016/679 Datenschutz-Grundverordnung | BSI-C5-Testat Typ 2 | Geprüfter Trusted Cloud Service | IDW PS 951 Typ 2 (ISAE 3402) geprüfter Dienstleister | Zertifizierung von Rechenzentren nach DIN EN 50600

Myra Security is the new benchmark for global IT security

Myra technology monitors, analyzes, and filters malicious internet traffic before virtual attacks can do any real harm. Our certified Security-as-a-Service platform protects your digital business processes from a wide range of risks, such as DDoS attacks, bot networks, and attacks on databases.